**U.S. Department of Justice**

*United States Attorney*
*Southern District of New York*

*Jacob K. Javitz Federal Building*
*26 Federal Plaza*
*New York, New York 10278*

March 10, 2025

**BY ECF**

The Honorable Jeannette A. Vargas
United States District Court
Southern District of New York
40 Foley Square
New York, New York 10007

**Re: *United States v. Ho*, 25 Cr. 3 (JAV)**

Dear Judge Vargas:

The Government respectfully submits this motion, pursuant to Federal Rule of Criminal Procedure 16(d)(1) and Title 18, United States Code, Section 1835(a), for entry of the attached proposed protective order governing the disclosure of proprietary and trade secrets to the defense (the "Proposed Protective Order"). The Government understands that the defense objects to certain provisions of the Proposed Protective Order, as described below, and respectfully requests that the Court resolve the parties' dispute over the contested provisions. Because those provisions are necessary to protect the victim from further harm, and the terms of the Proposed Protective Order are not otherwise disputed, the Government requests that the Court enter the Proposed Protective Order, attached hereto, or schedule a conference to address the matter.

## I. Offense Conduct

Firm-1 is a global quantitative trading firm, which trades in equities and other securities in exchanges located in the United States and abroad. Indictment ¶ 1. Firm-1's competitive advantage comes in large part from its proprietary source code ("Firm-1's Source Code"), which allows Firm-1 to make extremely rapid execution of a high volume of trades. Indictment ¶¶ 1, 5. Firm-1 spent years developing the Source Code almost entirely in-house at the cost of over a billion dollars. Indictment ¶ 7. Specifically, Firm-1 developed a library of Atoms, which are the building blocks and foundation of Firm-1's Source Code, each of which has specific functions, ranging from computational functions to price-predicting computations. Indictment ¶ 8. The Atoms are used to build Alphas, which are Firm-1's predictive formulas that make price predictions based on real-time market data. *Id.*

Because the linchpin to Firm-1's success is keeping its proprietary information secret, Firm-1 places a huge emphasis on the protection of is proprietary and trade secret information, including, most crucially, its Source Code. Indictment ¶ 9. For example, all employees are required to sign employment contracts that spell out their obligations to maintain the confidentiality of Firm-1 proprietary information and contain non-compete clauses. Indictment ¶

9(c). Employees also receive regular trainings on the importance of protecting Firm-1 trade secrets. Indictment ¶ 9(d).

In 2019, Firm-1 offered Cheuk Fung Richard Ho, the defendant, a job as a quantitative researcher and developer. Indictment ¶ 10. Due to the nature of his job, he was given nearly complete access to Firm-1's Source Code. *Id.* Like other similarly-situated employees, Ho signed an employment contract that, among other things, included a non-compete agreement, in which Ho acknowledged the central importance of proprietary information to Firm-1 and agreed that all proprietary information provided to the defendant and developed by him is the sole and exclusive property of Firm-1. Indictment ¶ 11. The defendant further agreed to not use proprietary information for his personal benefit or to compete with Firm-1. Indictment ¶ 11(b).

Despite the defendant's acknowledge his obligations to maintain the confidentiality of Firm-1's proprietary information and to not misappropriate Firm-1's proprietary information for his own personal benefit, evidence shows that the defendant did exactly that.

In the winter and spring of 2021, while still employed at Firm-1, the defendant secretly started Firm-2, another quantitative trading firm in partnership with one of Firm-1's competitors ("Firm-3"). Indictment ¶ 2, 13. By May 2021, again still employed at Firm-1, he recruited a software engineer, Engineer-1, to work for him at Firm-2. Indictment ¶ 13. Engineer-1 had also worked at Firm-1 until just two months prior, in March 2021. *Id.*

On July 6, 2021, the defendant sent Firm-1 a notice of resignation. Indictment ¶ 15. By then, the defendant had already invited a second engineer, Engineer-2, to the defendant's home to help develop Firm-2's source code. Indictment ¶ 16. In fact, a day after the defendant tendered his notice of resignation, and while he still had access to Firm-2 source code, the defendant accessed Firm-1's systems in front of Engineer-2 and showed him a Firm-1 feature that, among other things, visualizes market data, and told Engineer-2 that he wanted to create something similar for Firm-2. *Id.*

A review of the source code for Firm-2 (the "Firm-2 Source Code") reveals that the Firm-2 Source Code copied portions of Firm-1's Source Code, including Firm-1's Atoms and Alphas. Indictment ¶ 18. Indeed, Ho maintained an index (the "Index") within the Firm-2 Source Code directory that contained the unique names and parameters of numerous Firm-1 Atoms. Indictment ¶ 19. Tellingly, Ho refused to share the Index with Engineer-1, who had worked at Firm-1. *Id.* When Engineer-1 finally gained access to the Index and discovered numerous names of Firm-1 Atoms on the Index, Engineer-1 and two other employees quit Firm-2. Indictment ¶ 23.

In addition to unlawfully copying Firm-1 Source Code for his own benefit, the defendant also undertook a series of deceitful actions aimed at covering up his wrongdoing. At various points in or about approximately 2022 and 2023, when Engineer-1 started asking questions after discovering pieces of code that resembled code at Firm-1 in both name and function, Ho changed the name of the code and implemented a different version of the code that was publicly available. Indictment ¶ 21. In 2022 and 2023, despite an obligation under the defendant's non-compete agreement with Firm-1 to report his employment plans, the defendant did not report that he

started Firm-2; and when Firm-1 asked the defendant specifically about Firm-2, the defendant lied about Firm-2's trading activities. Indictment ¶ 20. Then, in 2023, when Firm-1 confronted the defendant regarding his founding of Firm-2, the defendant directed his employees to change the retention settings for Firm-2's internal messages such that they automatically deleted after a certain period of time and to delete the source code history for the Firm-2 Source Code. Indictment ¶ 22.

In short, the offense conduct demonstrates that the defendant is capable of sidestepping known obligations to protect the confidentiality of Firm-1's proprietary information for his own gain, and that he was willing to deceive Firm-1 and his own employees and to destroy evidence in order to cover his own wrongdoing.

## II. Applicable Law

### 1. Federal Rule of Criminal Procedure 16

Pursuant to Federal Rule of Criminal Procedure 16, "[a]t any time the court may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief." Fed. R. Crim. P. 16(d)(1). This Court has broad discretion to fashion appropriate protective orders related to discovery and disclosure in criminal cases. *See* Fed. R. Crim. P. 16(d)(1); *United States v. Delia*, 944 F.2d 1010, 1018 (2d Cir. 1991). Indeed, "the Supreme Court has held that 'the trial court can and should, where appropriate, place a defendant and his counsel under enforceable orders against unwarranted disclosure of the materials which they may be entitled to inspect." *United States v. Smith*, 985 F. Supp. 2d 506, 521 (S.D.N.Y. 2013) (quoting *Alderman v. United States*, 394 U.S. 165, 185 (1969)). The considerations that the Court may take into account include "the safety of witnesses and others," "a particular danger [of] perjury or witness intimidation," and "the protection of business enterprises from economic reprisals." Advisory Committee Notes to Fed. R. Crim. P. 16(d).

### 2. Economic Espionage Act

Congress enacted the Economic Espionage Act of 1996 (the "EEA") "to prevent economic espionage and to maintain the confidentiality of trade secrets." *United States v. Hsu*, 155 F.3d 189, 202 (3d Cir. 1998). Congress intended the statute to reach "virtually every form of illegal industrial espionage," including not only spying by foreign governments and corporate espionage between two competing companies, but also "the disgruntled former employee who walks out of his former company with a computer diskette full of engineering schematics.'" *Id.* at 201 (quoting H.R. Rep. No. 104-788, at 5 (1996)). Rather than simply define new criminal offenses, however, Congress created a "comprehensive federal criminal statute" intended to "better facilitate the investigation and prosecution of th[e] crime" and thereby "serve as a powerful deterrent." H.R. Rep. No. 104- 788, at 7.

Trade secrets derive their economic value from not being known competitors or the public. *See* 18 U.S.C. § 1839(3) (defining "trade secret"). Thus, any public disclosure of a trade secret poses a substantial risk that the trade secret's value to its owner will be significantly diminished, if not destroyed outright. As part of the EEA's comprehensive design, Congress

sought to prevent the public disclosure of trade secrets at issue in criminal prosecutions for theft of trade secrets. Thus, Congress enacted a provision explicitly mandating that trial courts "*shall* enter such orders and take other action as may be necessary and appropriate *to preserve the confidentiality of trade secrets*, consistent with the requirements of the Federal Rules of Criminal and Civil Procedure, the Federal Rules of Evidence, and all other applicable laws." 18 U.S.C. § 1835(a) (emphasis added). Section 1835 was enacted "to preserve the confidentiality of alleged proprietary economic information during legal proceedings under the Act consistent with existing rules of criminal procedure and evidence, and other applicable laws." S. Rep. No. 104-359, at 17 (1996). Congress went even further to protect the rights of trade secret owners in the context of criminal discovery when it supplemented Section 1835 in the Defend Trade Secrets Act of 2016. Congress expressly provided that a court "may not authorize or direct the disclosure of any information the owner asserts to be a trade secret unless the court allows the owner the opportunity to file a submission under seal that describes the interest of the owner in keeping the information confidential." 18 U.S.C. § 1835(b).

Congress enacted Section 1835 to advance two compelling interests. First, the provision was designed to "'preserve the confidential nature of the information and, hence, its value.'" *United States v. Ye*, 436 F.3d 1117, 1121 (9th Cir. 2006) (quoting H.R. Rep. No. 104-788, at 13); *cf. In re Iowa Freedom of Information Council*, 724 F.2d 658, 662 (8th Cir. 1983) ("Trade secrets are a peculiar kind of property. Their only value consists in their being kept private. If they are disclosed or revealed, they are destroyed."). Second, Congress sought to "encourage[] enforcement actions by protecting owners who might otherwise 'be reluctant to cooperate in prosecutions for fear of further exposing their trade secrets to public view, thus further devaluing or even destroying their worth.'" *Hsu*, 155 F.3d at 197 (quoting H.R. Rep. No. 104-788, at 13); *see also United States v. Yang*, 281 F.3d 534, 543 (6th Cir. 2002) (recognizing that "the purpose of the EEA was to provide a comprehensive tool for law enforcement personnel to use to fight theft of trade secrets," including with "the assistance of people willing to cooperate to catch and convict thieves of trade secrets"). Thus, Section 1835 "represent[s] a clear indication from Congress that trade secrets are to be protected to the fullest extent during EEA litigation." *Hsu*, 155 F.3d at 197.

As Section 1835 and the EEA's legislative history make clear, the protection of the confidentiality of a victim's trade secrets is such an overriding interest as to warrant limits on disclosure and other protective measures as appropriate. *See United States v. Roberts*, 08 Cr. 175, 2010 WL 1010000, at *5 (E.D. Tenn. Mar. 17, 2010) ("A certain absurdity exists in requiring [the victim] to publicly disclose the trade secrets at issue in a prosecution of the alleged theft and disclosure of those same trade secrets."). Not only do victims have a strong interest in not being re-victimized when their trade secrets are disclosed to the public and their competitors, but the Government has an interest in effective criminal enforcement under the EEA—one that encourages, rather than discourages, victims to come forward and report offenses.

## III. Discussion

The defendant's principle objections to the Government's Proposed Protective Order, attached herein as Exhibit A, are to (1) the inclusion of Attorney's Eyes Only ("AEO") and Attorney's Possession Only ("APO") designations (Proposed Protective Order ¶¶ 2, 3, 7, 8); (2)

the proposal to limit the defense's review of Proprietary Materials at an FBI facility and the concomitant restrictions regarding use of personal electronics and enforcement of the restrictions set forth therein (*Id.* ¶ 4, 9); and (3) the proposal that any defense expert seeking access to the Proprietary Materials must first disclose to the Court the expert's curriculum vitae so that the Government may have an opportunity to be heard on the proposed expert's potential conflicts of interest (*Id.* 9(h)). The Government respectfully submits that the Proposed Protective Order's inclusion of these provisions is amply supported by good cause, namely, to protect the victim from further harm, and that the Proposed Protective Order should be promptly entered.

First, the Government intends to use the AEO and/or APO designations sparingly, and has produced substantial discovery to date without invoking those provisions.[1] However, we believe that these categories may be necessary to protect records which may make reference to sensitive business information belonging to the victim or the identity of witnesses, and retaining these two categories of designation will preserve flexibility to expeditiously produce discovery without having to first seek a modification of the protective order. Entry of the Proposed Protective Order with these two designations does not prevent the defense from later disputing whether any particular document should rightfully be designated as either APO or AEO. Pursuant to Paragraph 11 of the proposed Protective Orders, if the defense disputes any of the Government's designations in this case, the defense may ultimately seek re-designation by the Court if the parties are unable to arrive at a resolution on consent. Courts in this district have routinely entered protective orders that set forth these two categories of designation, particularly in cases such as this which involved sensitive information.

Second, the Government respectfully submits that limiting the defense's review of Proprietary Material to an FBI facility is necessary in this case to protect the very trade secrets whose theft is already the subject of the charged conduct.

As set forth above, the crux of the case is whether the defendant misappropriated portion of Firm-1's Source Code when he was writing the source code for Firm-2. During the investigation, the Government obtained, pursuant to subpoenas, Firm-1 and Firm-2 Source Code, both of which contain Firm-1 trade secrets. The Government also obtained nearly 1 million documents from Firm-1, for which a narrow set of documents include proprietary information—such as discussions regarding particular portions of code—including emails and other documents that the defendant may have never seen before. The Government proposes that only Firm-1 and Firm-2 Source Code and a small subset of documents identified by Firm-1 to contain proprietary information—such as discussions regarding particular portions of code and other closely guarded information the disclosure of which could injure Firm-1's economic value—collectively identified as Proprietary Material be made available to the defense at a FBI Facility on a secured

[1] To date, the Government has made two productions of discovery that do not contain Proprietary Material or materials that would be designated as Attorney's Eyes Only and Attorney's Possession Only. These two productions consist of nearly all of the discovery materials currently in the Government's possession with the exception of materials received from Firm-1. Firm-1 initially produced nearly 1 million documents to the Government. Firm-1 is currently reviewing its documents to determine which contain Proprietary Material. The Government has been producing to the defense Firm-1 documents that are not Proprietary Materials on a rolling basis.

computer in a secure room without internet or network access to other computers and devices. Proposed Protective Order ¶ 9(a). The vast majority of discovery in this case have been and will be produced to the defense without these restrictions. This provision is tailored to address only those documents for which disclosure would substantially harm the value of Firm-1's intellectual property and Firm-1's competitive edge in the market. Moreover, the public has an interest in the adequate protection of Firm-1's proprietary information in this case. Disclosure of Firm-1's trade secrets to the public or to competitors—whether intentionally or inadvertent—would significantly hinder the Government's ability to effectively enforce the EEA in the future because other victims of theft of trade secrets would be discouraged from cooperating in the investigation and such prosecution of such crimes if it determined that materials they were required to turn over pursuant to subpoenas may later be disclosed to the public. Any value that victims of theft of trade secrets are trying to protect would thus be completely destroyed.

While the defense contests the Government's proposal on the handling of Proprietary Materials as overly restrictive, the Government respectfully disagrees. The defense's review of the Proprietary Material at a secure Government facility, using Government equipment that is not connected to the Internet, is the only way to adequately ensure that Firm-1's trade secret data is not lost, stolen, or otherwise distributed—whether intentionally or unintentionally. Even assuming that defense counsel, the defendant and others, such as defense experts, all act in good faith and do not intentionally disclose any of the Proprietary Material, use of the defense counsel's or the defendant's devices would require copying the Proprietary Material from Government systems to those devices. This copying would create the risk of potential inadvertent disclosure of the data in any number of scenarios, including but not limited to unauthorized access to the devices through system vulnerabilities (such as by password theft or undetected malware being installed on the devices in question); the devices themselves being lost or stolen; or accidental disclosure or transmittal of data.

The Government has also proposed ways to mitigate the burden on the defense. Though the Government is proposing as an initial matter that the Proprietary Materials be made available at the FBI Facility in New York, the Proposed Protective Order provides that the "Government shall promptly explore the viability of making some or all Proprietary material available for inspection, on the same terms and conditions as set forth herein, at the Federal Bureau of Investigation facility in another district." Proposed Protective Order ¶ 9(f). In addition, the Proposed Protective Order provides that the "Government will meet and confer in good faith with the defense regarding" any "specific software or accommodations" that the defense may need to examine the Proprietary Material. Proposed Protective Order ¶ 9(a). The availability of the AEO and APO designations also grant the Government flexibility to make some sensitive materials available to the defense under less restrictive conditions, if it is possible to do so while safeguarding the victim's interests. The Government will also make available a secured, air-gapped computer, on which the defense may take electronic notes if they so wish as they review the Proprietary Material. Proposed Protective Order ¶ 9(c).

Finally, to the extent that the Court agrees that the Government may make available Proprietary Materials only at FBI facilities, the Court should also enter the other concomitant restrictions regarding copying (Proposed Protective Order ¶ 9(b)); bringing in personal electronic devices (*Id.* ¶ 9(c)); and the Government's ability to enforce the restrictions by maintaining a log

of the names of individuals inspecting the Proprietary Material, visually monitoring through periodic spot checks of the activities of the people reviewing the Proprietary Materials, and reasonable searches of individuals inspecting the Proprietary Materials, upon reasonable cause, to ensure that there is no unauthorized recording, copying, or transmission of Proprietary Materials (*Id.* ¶ 9(e)). These concomitant restrictions are necessary for the same reasons that the Government believes that the Proprietary Materials may only be adequately guarded by keeping the materials on secured computers at a Government facility. The purpose of keeping the materials at a Government facility would be defeated if the defense were allowed to record, copy, or otherwise transmit the contents of the Proprietary Material, the risk of which is increased if the defense were permitted to bring their personal electronic devices (which is a restriction that generally applies to all non-FBI personnel entering FBI facilities), and if there is no enforcement mechanism.

The Government expects to designate as Proprietary Material only a small subset of discovery, including Firm-1 Source Code, Firm-2 Source Code, and limited other Firm-1 documents, some of which the defendant may have never previously seen, which discuss Firm-1 Source Code and other confidential and closely protected business secrets, the disclosure of which could seriously harm Firm-1's competitive edge. Protective Orders with provisions similar to the Proposed Protective Order here have been entered in other cases involving theft of trade secrets. *See, e.g., United States v. Zhang*, 17 Cr. 560 (JMF) (March 20, 2018) (Docket No. 75) (Judge Furman entering a Protective Order that limits defense review of Proprietary Materials to FBI facilities over defense objections); *United States v. Agrawal*, 10 Cr. 417 (JGK) (S.D.N.Y. July 16, 2010) (ECF No. 16) ("Protected Information" "shall be maintained in a safe and secure manner by the Government" and will be available to defense only at "Government offices" ); *see also United States v. Liu*, 16 Cr. 79 (E.D.Wis. July 15, 2016) (Docket No. 12) (any material designated a trade secret may be reviewed by defense "only at the Office of the United States Attorney or the Federal Bureau of Investigation Milwaukee Field Office); *United States v. Sinovel et al.*, 13 Cr. 84 (W.D. Wis. Feb. 5, 2016) (Docket No. 107) (making source code available to defense at the Milwaukee FBI office "on a secured computer in a secure room without internet access or network access to other computers"). Accordingly, the Court should enter the Proposed Protective Order because it is tailored to address these compelling interests while still preserving the defense's ability to inspect and review the proprietary material, including trade secrets, in preparing to defend the case.

Third, the Government believes it is necessary in a trade secrets case such as this that the Court and the Government has an opportunity to vet proposed defense experts for potential conflicts of interest. Proposed Protective Order 9(h). Central to the Proposed Protective Order is the core principle that Firm-1 should not be further harmed during the prosecution of this case through the disclosure of Firm-1 trade secrets and other proprietary information. Thus, to the extent that the defense intends to disclose Proprietary Materials to an expert, the Court and the Government should have an opportunity to confirm that the expert is not someone who will, once exposed to Firm-1's proprietary information, use that information in competition with Firm-1. This provision does not apply to experts whom the defense intends to only consult without sharing Firm-1 proprietary information. Absent such a provision, Firm-1 may be subject to an unacceptable risk that their trade secret and proprietary information could be shared with unidentified persons who are or will in the near future become direct competitors.

For these reasons, the Government respectfully submits that the proposed Protective Order should be entered by the Court.

Respectfully submitted,

MATTHEW PODOLSKY
Acting United States Attorney

by: */s/*
Ni Qian
Rushmi Bhaskaran
Assistant United States Attorneys
United States Attorney's Office for the
Southern District of New York
212-637-2364/ - 2439